Computational aspects of hyperelliptic curves

T. Shaska
Department of Mathematics,
University of California at Irvine
E-mail: tshaska@math.uci.edu

Abstract

We introduce a new approach of computing the automorphism group and the field of moduli of points $\mathfrak{p} = [C]$ in the moduli space of hyperelliptic curves $\mathcal{H}_g$. Further, we show that for every moduli point $\mathfrak{p} \in \mathcal{H}_g(L)$ such that the reduced automorphism group of $\mathfrak{p}$ has at least two involutions, there exists a representative C of the isomorphism class $\mathfrak{p}$ which is defined over L.

1 Introduction

The purpose of this note is to introduce some new techniques of computing the automorphism group and the field of moduli of genus g hyperelliptic curves. Former results by many authors have focused on hyperelliptic curves of small genus, see [8], [3], [7], [10], [12], et. al. We aim to find a method which would work for any genus.

Let C denote a genus g hyperelliptic curve defined over an algebraically closed field k of characteristic zero and $G := Aut(C)$ its automorphism group. We denote by $\mathcal{H}_g$ the moduli space of genus g hyperelliptic curves and by $\mathcal{L}_g$ the locus in $\mathcal{H}_g$ of hyperelliptic curves with extra involutions. $\mathcal{L}_g$ is a g-dimensional rational variety, see [6]. Equation 2 gives a normal form for curves in $\mathcal{L}_g$. This normal form depends on parameters $a_1, \dots, a_g \in k$, such that the discriminant of the right side $\Delta(a_1, \dots, a_g) \neq 0$. Dihedral invariants $(u_1, \dots, u_g)$ were introduced by Gutierrez and this author in [6]. The tuples $\mathfrak{u} = (\mathfrak{u}_1, \dots, u_g)$ (such that $\Delta_{\mathfrak{u}} \neq 0$) are in one-to-one correspondence with isomorphism classes of genus g hyperelliptic curves with automorphism group the Klein 4-group. Thus, dihedral invariants $u_1, \dots, u_g$ yield a birational parameterization of the locus $\mathcal{L}_g$. Computationally these invariants give an efficient way of determining a generic point of the moduli space $\mathcal{L}_g$. Normally, this is accomplished by invariants of $GL_2(k)$ acting on the space of binary forms of degree $2g+2$. These $GL_2(k)$-invariants are not known for $g \geq 3$. However, dihedral invariants are explicitly defined for all genera.

The full automorphism groups of hyperelliptic curves are determined in [2] and [1]. Most of these groups have non-hyperelliptic involutions (i.e., the corresponding curve is in $\mathcal{L}_g$). For each group G that occurs as full automorphism group of genus g curves one determines the G-locus in $\mathcal{L}_g$ in terms of the dihedral invariants. Given a genus g curve C we first determine if $C \in \mathcal{L}_g$. Then we compute its dihedral invariants and determine the locus $\mathcal{L}_G$ that they satisfy. This determines $Aut(C)$. Present algorithms of computing the automorphism group of a hyperelliptic curve $Y^2 = F(X)$ are based on computing the roots of $F(X)$ and then finding fractional linear transformations that permute these roots. The algorithm we propose requires only determining the normal form of C (i.e., Eq. 2). This requires solving a system of g-equations and four unknowns. For curves which have at least two involutions in their reduced automorphism group we find a nice condition on the dihedral invariants.

For $C \notin \mathcal{L}_g$ similar methods can be used. If $|Aut(C)| > 2$ and $C \notin \mathcal{L}_g$, then C has an automorphism of order N, where N is as in Lemma 3. For small genus these curves can be classified by ad-hoc methods. In general one needs to find invariants of such spaces for all $N > 2$ and implement similar methods as above. We intend this as the object of further research.

In section 4, we introduce how to compute the field of moduli of genus g hyperelliptic curves with automorphism group of order > 4. Let $\mathcal{M}_g$ (resp., $\mathcal{H}_g$) be the moduli space of algebraic curves (resp., hyperelliptic curves) of genus g defined over k and L a subfield of k. It is well known that $\mathcal{M}_g$ (resp., $\mathcal{H}_g$) is a $3g-3$ (resp., $2g-1$) dimensional variety. If C is a genus g curve defined over L, then clearly $[C] \in \mathcal{M}_g(L)$. However, the converse is not true. In other words, the moduli space $\mathcal{M}_g$ of algebraic curves of genus g is a coarse moduli space. The answer is not obvious if we restrict ourselves to the singular points of $\mathcal{M}_g$. Singular points of $\mathcal{M}_g$ (resp., $\mathcal{H}_g$) correspond to isomorphism classes of curves with nontrivial automorphism groups (resp., automorphism groups of order > 2). In general, we conjecture that for a singular point $\mathfrak{p} \in \mathcal{M}_g(L)$ (resp., $\mathfrak{p} \in \mathcal{H}_g(L)$) there is always a curve C defined over L which correspond to $\mathfrak{p}$. We focus on $\mathcal{H}_g$. A point $\mathfrak{p} = [C] \in \mathcal{H}_g$ is given by the g-tuple of dihedral invariants. We denote by $Aut(\mathfrak{p})$ the automorphism group of any representative C of $\mathfrak{p}$. More precisely, for hyperelliptic curves we conjecture the following:

Conjecture 1: *Let $\mathfrak{p} \in \mathcal{H}_g(L)$ such that $|Aut(\mathfrak{p})| > 2$. There exists a representative C of the isomorphism class $\mathfrak{p}$ which is defined over L.*

In this paper we show how dihedral invariants can be used to prove some special cases of this conjecture. A detailed discussion on this problem is intended in [11]. The condition $|Aut(\mathfrak{p})| > 2$ of the above conjecture can not be dropped. Determining exactly the points $\mathfrak{p} \in \mathcal{H}_g \setminus \mathcal{L}_g$ where such rational model C does not exist is still an open problem. For $g = 2$ Mestre (1991) found an algorithm which determines such points. It is based on classical invariants of binary sextics.

Notation: Throughout this paper k denotes an algebraically closed field of characteristic zero, g an integer ≥ 2, and C a hyperelliptic curve of genus g. $\mathcal{M}_g$ (resp., $\mathcal{H}_g$) is the moduli space of curves (resp., hyperelliptic curves) defined over k. Further, V_4 denotes the Klein 4-group and D_{2n} (resp., $\mathbb{Z}_n$) the dihedral group of order $2n$ (resp., cyclic group of order n).

2 Dihedral invariants of hyperelliptic curves

Let k be an algebraically closed field of characteristic zero and C be a genus g hyperelliptic curve given by the equation $Y^2 = F(X)$, where $\deg(F) = 2g+2$. Denote the function field of C by $K := k(X,Y)$. Then, $k(X)$ is the unique degree 2 genus zero subfield of K. We identify the places of $k(X)$ with the points of $\mathbb{P}^1 = k \cup \{\infty\}$ in the natural way (the place $X = \alpha$ gets identified with the point $\alpha \in \mathbb{P}^1$). Then, K is a quadratic extension field of $k(X)$ ramified exactly at $n = 2g+2$ places $\alpha_1, \dots, \alpha_n$ of $k(X)$. The corresponding places of K are called the *Weierstrass points* of K. Let $\mathcal{P} := \{\alpha_1, \dots, \alpha_n\}$. Thus, $K = k(X,Y)$, where

$$Y^2 = \prod_{\alpha \in \mathcal{P},\ \alpha \neq \infty} (X - \alpha). \tag{1}$$

Let $G = Aut(K/k)$. Since $k(X)$ is the only genus 0 subfield of degree 2 of K, then G fixes $k(X)$. Thus, $G_0 := Gal(K/k(X)) = \langle z_0 \rangle$, with $z_0^2 = 1$, is central in G. We call **the reduced automorphism group** of K the group $\overline{G} := G/G_0$. Then, $\overline{G}$ is naturally isomorphic to the subgroup of $Aut(k(X)/k)$ induced by G. We have a natural isomorphism $\Gamma := PGL_2(k) \to Aut(k(X)/k)$. The action of Γ on the places of $k(X)$ corresponds under the above identification to the usual action on $\mathbb{P}^1$ by fractional linear transformations $t \mapsto \frac{at+b}{ct+d}$. Further, G permutes $\alpha_1, \dots, \alpha_n$. This yields an embedding $\overline{G} \hookrightarrow S_n$.

Because K is the unique degree 2 extension of $k(X)$ ramified exactly at $\alpha_1, \dots, \alpha_n$, each automorphism of $k(X)$ permuting these n places extends to an automorphism of K. Thus, $\overline{G}$ is the stabilizer in $Aut(k(X)/k)$ of the set $\mathcal{P}$. Hence under the isomorphism $\Gamma \mapsto Aut(k(X)/k)$, $\overline{G}$ corresponds to the stabilizer $\Gamma_{\mathcal{P}}$ in Γ of the n-set $\mathcal{P}$.

An extra involution of K is an involution in G which is different from z_0 (the hyperelliptic involution). If z_1 is an extra involution and z_0 the hyperelliptic one, then $z_2 := z_0\, z_1$ is another extra involution. So the extra involutions come naturally in pairs. Suppose z_1 is an extra involution of K. Let $z_2 := z_1\, z_0$, where z_0 is the hyperelliptic involution. Then $K = k(X,Y)$ with equation

$$Y^2 = X^{2g+2} + a_g X^{2g} + \cdots + a_1 X^2 + 1 \tag{2}$$

see [6]. The dihedral group $H := D_{2g+2} = \langle \tau_1, \tau_2 \rangle$ acts on $k(a_1, \dots, a_g)$ as follows:

$$\begin{aligned} \tau_1 : \quad & a_i \quad \to \varepsilon^{2i} a_i, \qquad for \quad i = 1, \dots, g \\ \tau_2 : \quad & a_i \quad \to a_{g+1-i}, \qquad for \quad i = 1, \dots, [\frac{g+1}{2}] \end{aligned}$$

The fixed field $k(a_1, \dots, a_g)^H$ is the same as the function field of the variety $\mathcal{L}_g$. The invariants of such action are

$$u_i := a_1^{g-i+1}\, a_i \, + \, a_g^{g-i+1}\, a_{g-i+1}, \quad for \quad 1 \le i \le g \tag{3}$$

and are called **dihedral invariants** for the genus g and the tuple

$$\mathfrak{u} := (u_1, \dots, u_g)$$

is called the **tuple of dihedral invariants**, see [6] for details.

It is easily seen that $\mathfrak{u} = 0$ if and only if $a_1 = a_g = 0$. In this case replacing a_1, a_g by a_2, a_{g-1} in the formula above would give new invariants. In [6] it is shown that $k(\mathcal{L}_g) = k(u_1, \dots, u_g)$. The $(2g+2)$-degree field extension $k(a_1, \dots, a_g)/k(u_1, \dots, u_g)$ has equation

$$2^{g+1}\, a_g^{2g+2} - 2^{g+1}\, u_1\, a_g^{g+1} + u_g^{g+1} = 0 \tag{4}$$

and the map

$$\begin{array}{lll} \Phi: & k \setminus \{\Delta \neq 0\} & \to \mathcal{L}_g \\ & (a_1, \dots, a_g) & \to (u_1, \dots, u_g) \end{array}$$

has Jacobian zero exactly on points which correspond to curves $C \in \mathcal{L}_g$ such that $V_4 \hookrightarrow \overline{G}$.

3 Automorphism groups

In this section we suggest an algorithm for computing the full automorphism group of hyperelliptic curves. Let C be a genus g hyperelliptic curve with equation $Y^2 = F(X)$ where $\deg(F) = 2g + 2$. Existing algorithms are based on finding all automorphisms of C. Instead, we search for only one automorphism (non-hyperelliptic) of C of order N. Most of the time $N = 2$ is enough since the majority of groups of order > 2 that occur as full automorphism groups have non-hyperelliptic involutions. It is well known that the order of a non-trivial automorphism of a hyperelliptic curve is $2 \leq N \leq 2(2g + 1)$, where $2(2g + 1)$ is known as the Wiman's bound.

If an automorphism of order $N = 2$ exists then $C \in \mathcal{L}_g$ and we use dihedral invariants to determine the automorphism group. We illustrate with curves of small genus.

The case $g = 2$ has been studied in [12]. Every point in $\mathcal{M}_2$ is a triple (i_1, i_2, i_3) of absolute invariants. We state the results of [12] without proofs.

Lemma 1. *Let C be a genus 2 curve such that $G := Aut(C)$ has an extra involution and $\mathfrak{u} = (u_1, u_2)$ its dihedral invariants. Then,*

a) $G \cong \mathbb{Z}_3 \rtimes D_8$ if and only if $(u_1, u_2) = (0, 0)$ or $(u_1, u_2) = (6750, 450)$.

b) $G \cong GL_2(3)$ if and only if $(u_1, u_2) = (-250, 50)$.

c) $G \cong D_{12}$ if and only if $u_2^2 - 220u_2 - 16u_1 + 4500 = 0$, for $u_2 \neq 18, 140 + 60\sqrt{5}, 50$.

d) $G \cong D_8$ if and only if $2u_1^2 - u_2^3 = 0$, for $u_2 \neq 2, 18, 0, 50, 450$. Cases $u_2 = 0, 450$ and $u = 50$ are reduced to cases a) and b) respectively.

The mapping $\Phi : (u_1, u_2) \to (i_1, i_2, i_3)$, gives a birational parameterization of $\mathcal{L}_2$. The fibers of Φ of cardinality > 1 correspond to those curves C with $|Aut(C)| > 4$. Dihedral invariants u_1, u_2 are given explicitly as rational functions of i_1, i_2, i_3. The curve $Y^2 = X^6 - X$ is the only genus 2 curve (up to isomorphism) which has extra automorphisms and is not in $\mathcal{L}_2$. The automorphism group in this case is $\mathbb{Z}_{10}$, see [12]. Thus, if $C \in \mathcal{L}_2$ we determine $Aut(C)$ via Lemma 3.1., otherwise C is isomorphic to $Y^2 = X^6 - X$ or $Aut(C) \cong \mathbb{Z}_2$.

The case $g = 3$ is given as an application in [6]. Let $C \in \mathcal{L}_3$ with equation as in Eq. 2. Dihedral invariants are $u_1 = a_1^4 + a_3^4, u_2 = (a_1^2 + a_3^2)a_2, u_3 = 2a_1a_3$. The analogue of Lemma 3.1 is proved in [6] for $g = 3$.

This technique can be used successfully for all g. We have implemented programs that determine $Aut(C)$ for $C \in \mathcal{L}_g$ and for $g = 2, 3, 4, 5, 6$. In order to compute the automorphism group of a curve $C \in \mathcal{L}_g$ we transform this curve to its normal form (i.e., Eq. 2) and then compute its dihedral invariants. If these invariants satisfy any locus $\mathcal{L}_G$ then the automorphism group is G, otherwise the automorphism group is V_4. The following lemma determines a nice condition for $\overline{G}$ to have at least two involutions.

Lemma 2. *For a curve $C \in \mathcal{L}_g$ the reduced automorphism group has at least two involutions if and only if*

$$(2^{g-1}u_1^2 + u_g^{g+1})\,(2^{g-1}u_1^2 - u_g^{g+1}) = 0 \tag{5}$$

Proof. Let $C \in \mathcal{L}_g$. Then, there is an involution $z_1 \in \bar{G}$ which fixes no Weierstrass points of C, see the proof of lemma 1 in [6]. Thus, $z_1(X) = -X$. Let $z_2 \neq z_1$ be another involution in $\bar{G}$. Since, $z_2 \neq z_1$ then $z_2(X) = \frac{m}{X}$, where $m^2 = 1$. Then, $V_4 = \langle z_1, z_2 \rangle \hookrightarrow \bar{G}$ and z_2 or $z_1\, z_2$ is the transformation $X \to \frac{1}{X}$, say $z_2(X) = \frac{1}{X}$. If g is odd we have $\mathcal{P} = \{\pm\alpha_1, \pm\frac{1}{\alpha_1}, \dots, \pm\alpha_n, \pm\frac{1}{\alpha_n}\}$, where $n = [\frac{g+1}{2}]$, otherwise $\mathcal{P}$ contains also two points $\pm P$. Thus, $\pm P$ can be either fixed or permuted by $z_2(X) = \frac{1}{X}$. Hence, they are ± 1 or $\pm I$, where $I^2 = 1$. The equation of C is given by

$$\begin{aligned} Y^2 = & \prod_{i=1}^{n}(X^4 - \lambda_i X^2 + 1), \quad \textit{if } g \textit{ is odd} \\ Y^2 = & (X^2 \pm 1)\prod_{i=1}^{n}(X^4 - \lambda_i X^2 + 1), \quad \textit{if } g \textit{ is even.} \end{aligned}$$

Let $s := \lambda_1 + \dots + \lambda_n$. If g is odd then $a_1 = a_g = -s$. Then, $u_1 = 2s^{g+1}$ and $u_g = 2s^2$ and they satisfy Eq. 5. If $z_2(X) = \frac{1}{X}$ fixes two points of $\mathcal{P}$ then one of the factors of the equation is $X^4 - 1$. Then, $a_1 = (-1)^{\frac{1}{g+1}}\, s$ and $a_g = (-1)^{\frac{1}{g+1}}\, s$. Hence, $a_g^{g+1} = a_g^{g+1} = -s^{g+1}$ and $u_1 = -2s^{g+1}$, $u_g = -2s^2$. Then, $2^{g-1}u_1^2 + u_g^{g+1} = 0$.

If g is even and $\{\pm 1\} \subset \mathcal{P}$ then $a_1 = a_g = s + 1$. If $\{\pm I\} \subset \mathcal{P}$ then $a_1 = a_g = 1 - s$. In both cases $2^{g-1}u_1^2 - u_g^{g+1} = 0$. The converse goes similarly. □

Remark 1. *If $2^{g-1}u_1^2 + u_g^{g+1} = 0$, then one of the involutions z_2, $z_1 z_2$ of $\bar{G}$ lifts to an element of order 4 in G. If $2^{g-1}u_1^2 - u_g^{g+1} = 0$ both of them lift to involutions in G.*

For $C \notin \mathcal{L}_g$ we check if C has automorphisms of order $3 \leq N \leq 2(2g+1)$, see Wiman [15]. The following lemma is a consequence of [2] and gives possible values for N. We only sketch the proof.

Lemma 3. *Let C be a genus g hyperelliptic curve with an automorphism of order $N > 2$. Then either $N = 3, 4$ or one of the following holds;*
i) $N|(2g+1)$ or $N|2g$ and $N < g$ (then $Aut(C) \cong \mathbb{Z}_{2N}$)
ii) $N|2g$ and N is an even number such that $6 \leq N \leq 2g-2$.
iii) $N = 4N'$ such that $N'|g$ and $N' < g$.

Proof. Let C be a genus g hyperelliptic curve with extra automorphisms such that $C \notin \mathcal{L}_g$. Then, the automorphism group of C is isomorphic to one of the following: $SL_2(3)$, $SL_2(5)$, W_3, $H_{N/2}$, $U_{N/2}$, $G_{N/2}$, $\mathbb{Z}_{2N}$ where $N \,|\, 2g+1$ or $N \,|\, 2g$ and $N < g$; see [2] for definitions of these groups. All other groups listed in Table 2 in [2] contain at least two involutions, hence they correspond to curves in $\mathcal{L}_g$. The only groups in the above list that might not contain an element of order 2, 3, or 4 are $U_{N/2}$, $G_{N/2}$. The group $G_{N/2}$ (resp., $U_{N/2}$) has an element of order N where N is as above.

□

To have a complete algorithm that works for any $g \geq 2$, one needs to classify (up to isomorphism) curves of genus g which are not in the locus $\mathcal{L}_g$. In order to do this, we need invariants which classify isomorphism classes of curves with an automorphism of order $N > 2$. However, for small genus ad-hoc methods can be used to identify such groups.

4 Field of moduli

In this section we introduce a method to compute the field of moduli of hyperelliptic curves with extra automorphisms. Until recently this was an open problem even for $g = 2$. Further, we state some open questions for higher genus and prove Conjecture 1 for $\mathfrak{p} \in \mathcal{H}_g$ such that the reduced automorphism group of $\mathfrak{p}$ has at least two involutions.

Let C be a genus g hyperelliptic curve defined over k. We can write the equation of C as follows

$$Y^2 = X(X-1)(X^{2g-1} + c_{2g-2}X^{2g-2} + \cdots + c_1 X + c_0)$$

where the discriminant Δ of the right side is nonzero. Then, there is a map

$$\begin{aligned} \Phi_1 : \quad & k^{2g-1} \setminus \{\Delta \neq 0\} \to \mathcal{H}_g \\ & (c_0, \ldots, c_{2g-2}) \to \mathfrak{p} = [C] \end{aligned}$$

of degree $d = 4g(g+1)(2g+1)$. We denote by J_Φ the Jacobian matrix of a map Φ. Then Conjecture 1 can be stated as follows:

Conjecture 2: *For each $\mathfrak{p}$ in the locus $\det(J_{\Phi_1}) = 0$ such that $\mathfrak{p} \in \mathcal{H}_g(L)$ there exists a representative C of the isomorphism class $\mathfrak{p}$ which is defined over L.*

For $g = 2$ this conjecture is a theorem as shown in [3]. The main result in [3] is to prove the case when automorphism group is V_4. A method of Mestre is generalized which uses covariants of order 2 of binary sextics and a result of Clebsch. Such a method probably could be generalized to higher genus as claimed by Mestre [8] and Weber [14].

Remark 2. *There is a mistake in the proof of Theorem 2 in [3]. In other words, the proof is incorrect when the Clebsch invariant $C_{10} = 0$. However, it can easily be fixed. A correct version of the algorithm has been implemented in Magma by P. van Wamelen.*

For $g = 3$ the conjecture is proven by Gutierrez and this author for all points $\mathfrak{p}$ with $|Aut(\mathfrak{p})| > 4$, see [6]. The proof uses dihedral invariants of hyperelliptic curves. A generalization of the method used in [8], [14] for $\mathfrak{p} \in \mathcal{H}_3$ such that $Aut(\mathfrak{p}) \cong V_4$ would complete the case $g = 3$.

Next we focus on the locus $\mathcal{L}_g$. Let $C \in \mathcal{L}_g$. Then, C can be written in the normal form as in equation 2. The map

$$\begin{aligned} \Phi : \quad & k^g \setminus \{\Delta \neq 0\} \to \mathcal{L}_g \\ & (a_1, \dots, a_g) \to (u_1, \dots, u_g) \end{aligned}$$

has degree $d = 2g + 2$. We ask a similar question as in Conjecture 2. Let $\mathfrak{p}$ be in the locus $\det(J_{\Phi_1}) = 0$ such that $\mathfrak{p} \in \mathcal{H}_g(L)$. Is there a representative C of the isomorphism class $\mathfrak{p}$ which is defined over L?

The determinant of the Jacobian matrix is

$$\det(J_\Phi) = (2^{g-1}u_1^2 + u_g^{g+1})\,(2^{g-1}u_1^2 - u_g^{g+1}).$$

The locus $\det(J_\Phi) = 0$ corresponds exactly to the hyperelliptic curves with $V_4 \hookrightarrow \bar{G}$ as shown by Lemma 3.2.

Theorem 1. *For each $\mathfrak{p}$ in the locus $\det(J_\Phi) = 0$ such that $\mathfrak{p} \in \mathcal{H}_g(L)$ there exists a representative C of the isomorphism class $\mathfrak{p}$ which is defined over L. Moreover, the equation of C over L is given by*

$$C: \quad Y^2 = u_1 X^{2g+2} + u_1 X^{2g} + u_2 X^{2g-2} + \cdots \pm u_g X^2 + 2, \tag{6}$$

where the coefficient of X^2 is u_g (resp., $-u_g$) when $2^{g-1}u_1^2 - u_g^{g+1} = 0$ (resp., $2^{g-1}u_1^2 + u_g^{g+1} = 0$).

Proof. Let $\mathfrak{p} = (u_1, \dots, u_g) \in \mathcal{L}_g(L)$ such that $2^{g-1}u_1^2 - u_g^{g+1} = 0$. All we need to show is that the dihedral invariants of C satisfy the locus $\det(J_\Phi) = 0$. By the appropriate transformation C can be written as

$$Y^2 = X^{2g+2} + (\frac{u_1}{2})^{\frac{1}{g+1}} \cdot X^{2g} + \sum_{i=1}^{g-1} \frac{u_{g+1-i}}{u_1} \cdot (\frac{u_1}{2})^{\frac{g+1-i}{g+1}} \cdot X^{2i} + 1.$$

Then, its dihedral invariants are

$$u_1(C) = \frac{u_1}{2} + (\frac{u_g}{u_1})^{g+1} \cdot (\frac{u_1}{2})^g = \frac{2^{g-1}u_1^2 + u_g^{g+1}}{2^g u_1}, \quad u_g(C) = u_g.$$

Substituting $u_g^{g+1} = 2^{g-1}u_1^2$ we get $u_1(C) = u_1$. Thus, C is in the isomorphism class determined by $\mathfrak{p}$ and defined over L.

Let $\mathfrak{p} = (u_1, \dots, u_g) \in \mathcal{L}_g(L)$ such that $2^{g-1}u_1^2 + u_g^{g+1} = 0$. This case occurs only when g is odd, see the proof of Lemma 3.2. We transform C as above and have $u_1(C) = u_1$ and $u_g(C) = -u_g$. They are the other tuple $(u_1, ..., -u_g)$ which correspond to $\mathfrak{p}$. This completes the proof.

□

The following is a consequence of Lemma 3.2. and Theorem 4.1.

Corollary 1. *Conjecture 1 holds for all $p \in \mathcal{L}_g$ such that the reduced automorphism group of $\mathfrak{p}$ has at least two involutions.*

5 Closing remarks

Conjecture 1 was stated for the first time during a talk of the author in ANTS V, see [9]. It can be generalized to $\mathcal{M}_g$ instead of $\mathcal{H}_g$. However, little is known about the loci $\mathcal{M}_G$ (i.e., locus of curves in $\mathcal{M}_G$ with full automorphism group G). In [7] we introduce an algorithm that would classify such groups G for all g and give a complete list of "large" groups for $g \leq 10$. However, finding invariants that classify curves with automorphism group G is not an easy task, since the equations describing non-hyperelliptic curves are more complicated then the hyperelliptic case. A more theoretical approach on singular points of $\mathcal{M}_g$ probably would produce better results on Conjecture 1. At this time we are not aware of any such results.

Our approach would work (with necessary adjustments) even in positive characteristic. However, the goal of this note was to introduce such method rather than explore it to the full extent.

Computationally, dihedral invariants give an efficient way of determining a point of the moduli space $\mathcal{L}_g$. Using such invariants in positive characteristic could have applications in the arithmetic of hyperelliptic curves, including cryptography.

Acknowledgments

This paper was written during a visit at the University of Florida. I want to thank the Department of Mathematics at the University of Florida for their hospitality.

References

[1] R. Brandt and H. Stichtenoch, Die Automorphismengrupenn hyperelliptischer Kurven. *Manuscripta Math* **55** (1986), no. 1, 83–92.

[2] E. Bujalance, J.M. Gamboa, G. Gromadzki, The full automorphism groups of hyperelliptic Riemann surfaces, *Manuscripta Math.* **79** (1993), no. 3-4, 267–282.

[3] G. Cardona and J. Quer, Field of moduli and field of definition for curves of genus 2, Article math.NT/0207015.

[4] A. Clebsch, Theorie der Binären Algebraischen Formen, Verlag von B.G. Teubner, Leipzig (1872).

[5] P. Débes and M. Emsalem, On fields of moduli of curves. J. Algebra 211 (1999), no. 1, 42–56.

[6] J. Gutierrez and T. Shaska, Hyperelliptic curves with extra involutions, 2002, (submitted).

[7] K. Magaard, T. Shaska, S. Shpectorov, and H. Völklein, The locus of curves with prescribed automorphism group, *RIMS Series*, Communications in Arithmetic Fundamental Groups and Galois Theory, ed. H. Nakamura, vol. 6, pg. 112-141, (2002).

[8] P. Mestre, Construction de courbes de genre 2 á partir de leurs modules. In T. Mora and C. Traverso, editors, *Effective methods in algebraic geometry*, volume 94. *Prog. Math.*, 313-334. Birkhäuser, 1991. Proc. Congress in Livorno, Italy, April 17-21, (1990).

[9] T. Shaska, Genus 2 curves with (3,3)-split Jacobian and large automorphism group, LNCS, vol. **2369**, (2002) pg. 205-218.

[10] T. Shaska, Genus 2 fields with degree 3 elliptic subfields, Forum Math., 2002, (in press).

[11] T. Shaska, Field of moduli of hyperelliptic curves (in preparation).

[12] T. Shaska and H. Völklein, Elliptic Subfields and automorphisms of genus 2 function fields. *Algebra and Algebraic Geometry with Applications*, LNCS, (2002), (in press).

[13] T. Shioda, Constructing curves with high rank via symmetry. Amer. J. Math. 120 (1998), no. 3, 551–566.

[14] H. J. Weber, Hyperelliptic simple factors of $J_0(N)$ with dimension at least 3. Experiment. Math. 6 (1997), no. 4, 273–287.

[15] A. Wiman, Über die hyperelliptischen Curven vom den Geschlechte $p = 4, 5$, und 6, welche eindeutige Transformationen in sich besitzen, *Bihang Kongl. Svenska Vetenskaps-Akademiens Handlingar* (1895), no. 21 (3), 1–41.